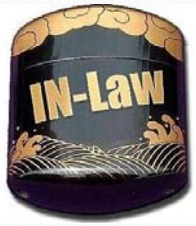
「情報セキュリティ対策と個人情報保護対策の違い」

「 PIMSの国際規格化に向けた状況と日本の対応」

佐藤　慶浩

「情報セキュリティ対策と個人情報保護対策の違い」の発表資料については、後日、学会ホームページ及び個人ホームページに掲載します。



http://in-law.jp/

yosihiro.com

http://よしひろ.com/speech/

情報セキュリティ対策と
個人情報保護対策の違い

2012年4月7日

日本ヒューレット・パッカード株式会社
個人情報保護対策室
佐藤　慶浩

©2010-2012

前回のアンケート結果から

■プライバシーや個人情報保護の対策には、情報流出対策や不正アクセス対策などの情報セキュリティ以外の対策として、どのようなことがあるか具体的に2つ以上ご存知ですか？

1．はい　　2．いいえ　　3．よくわからない

24名

「はい」の場合、
ご存知のものを2つだけ具体的にお書きください：

回答数　57名

正解＝13名 (23%)

日本ヒューレット・パッカード株式会社 ©2010-2012

個人情報保護対策

利用目的の特定

利用目的の本人への通知

利用についての本人からの同意獲得

第三者提供の際の本人からの同意獲得

本人からの要求（訂正、利用停止等）への対応

安全管理

など

日本ヒューレット・パッカード株式会社 ©2010-2012

弊社のﾏｰｹﾃｨﾝｸﾞ/営業担当者向けﾄﾚｰﾆﾝｸﾞ

HPの基本的な考え方
個人情報のライフサイクル
個人情報の利用
個人情報の安全管理措置

本日のスライド:
http://yosihiro.com/go/2012-02-20-aichi

日本ヒューレット・パッカード株式会社 ©2010

弊社のﾏｰｹﾃｨﾝｸﾞ/営業担当者向けﾄﾚｰﾆﾝｸﾞ トレーニング目的

以下の手順について、適切な手順を理解すること。

- お客様からお名前や連絡先（以下、お客様情報）を入力や記入していただき入手する際の手順
- 入手したお客様情報の保管と顧客データベースへの登録等の手順
- 顧客データベース等で管理しているお客様情報の利用手順
- お客様情報の入手に日本HP以外が関係（セミナーやイベントを他社と共催など）する場合の手順
- お客様情報をプロモーションで利用する際の手順

日本ヒューレット・パッカード株式会社 ©2010-2012

目次

お客様情報の取り扱い

- ●HPの基本的な考え方
- ●個人情報の入手
- ●個人情報の登録
- ●個人情報の利用
- ●個人情報の保管
- ●個人情報の通信・移送
- ●個人情報の廃棄・消去
- ●個人情報の提供（←共用・共同利用）
- ●個人情報を使ったプロモーション

日本ヒューレット・パッカード株式会社 ©2010-2012

個人情報のライフサイクル

日本ヒューレット・パッカード株式会社 ©2010

個人情報のライフサイクル

- 個人情報の属性
- 個人情報の入手
- 個人情報の登録
- 個人情報の保管
- 個人情報の通信・移送
- 個人情報の提供（←共用・共同利用）
- 個人情報の廃棄・消去

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の入手
一次的入手

利用目的の通知

セールス用途であれば「全社共通標準文言」を、それ以外であれば「業務連絡文言」を記載すること。

同一書面（同一ページ）に記載すること。

利用目的の同意（オプトイン）取得

電子メールアドレスとFAX番号を入手する場合には、*明示的な同意確認を得ること。*

住所と電話番号については、*必ずしも同意確認を得なくて構わない。*

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の入手
二次的入手

二次的入手の同意取得

一次的入手者からHPにお客様情報を提供することについて、
一次的入手者が、ご本人から同意を事前に得る必要がある。

その際に、
一次的入手と同じ「利用目的通知」「利用目的同意取得」をご本人に通知・確認する必要がある。

HPは、一次的入手者が上記を実施することについて「事前に」約束してもらう必要がある。

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の入手
同意（＝オプトイン：Opt-in）取得率の向上

お客様に同意をしていただきやすい文章で取得する必要がある。

「HPからの製品案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内を1ヶ月間に最大1回お送りしてもよろしいでしょうか？」

目的や頻度を限定すれば、同意取得率は向上する場合がある。

目的が広ければ、色々な目的に使えるが、同意取得率が低下する場合がある。

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の登録

お客様情報は、原則として お客様情報DB に登録しなければならない。

お客様情報DB の登録ガイドラインに従う。

利用目的の同意取得結果を正しく登録する。

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の保管

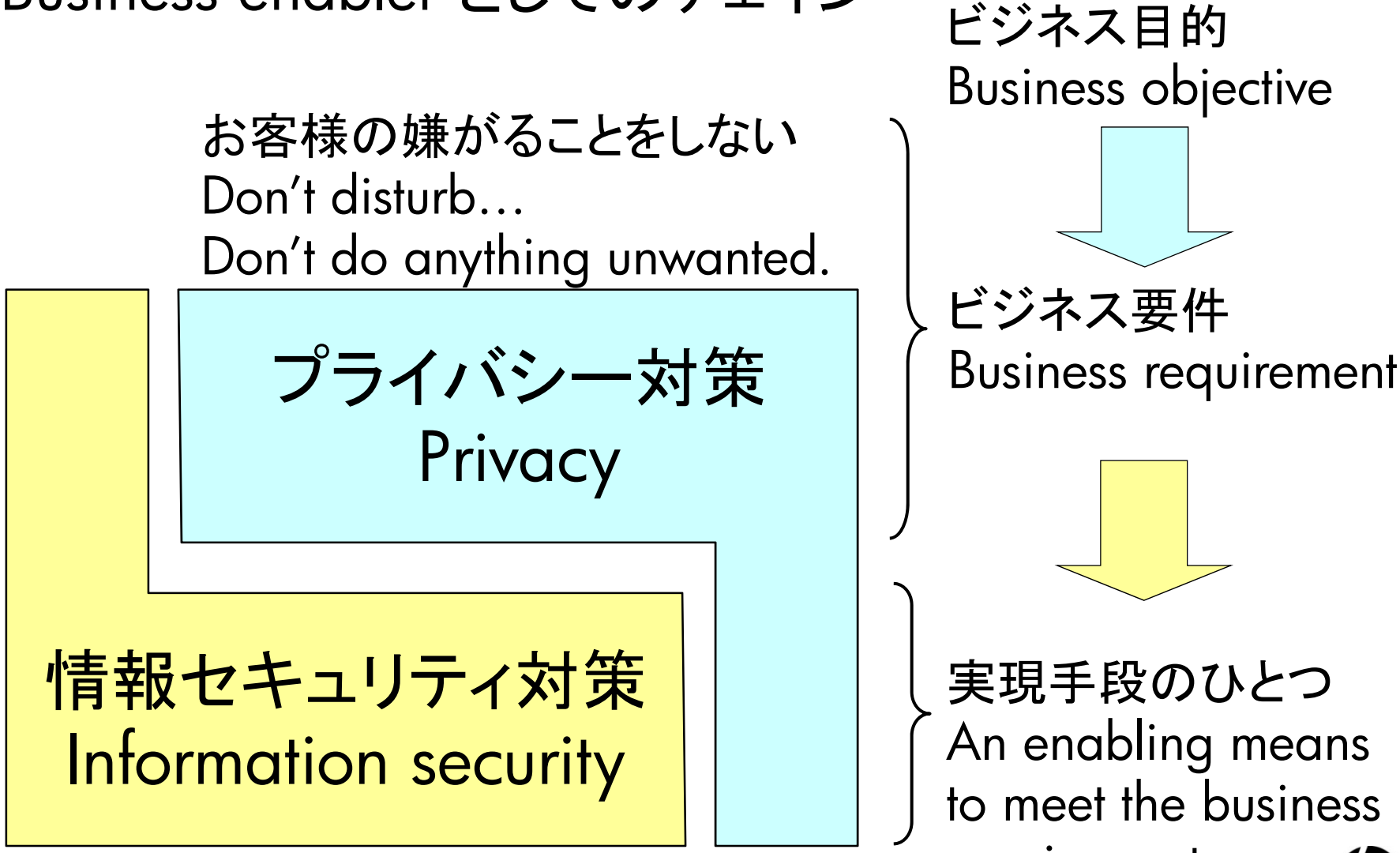
お客様情報の保管は一時的にだけ許される。

→恒常的（1ヶ月以上）保管は お客様情報DB に登録すること。

HP秘(HP Confidential)として保管する。

日本ヒューレット・パッカード株式会社 ©2010-2012

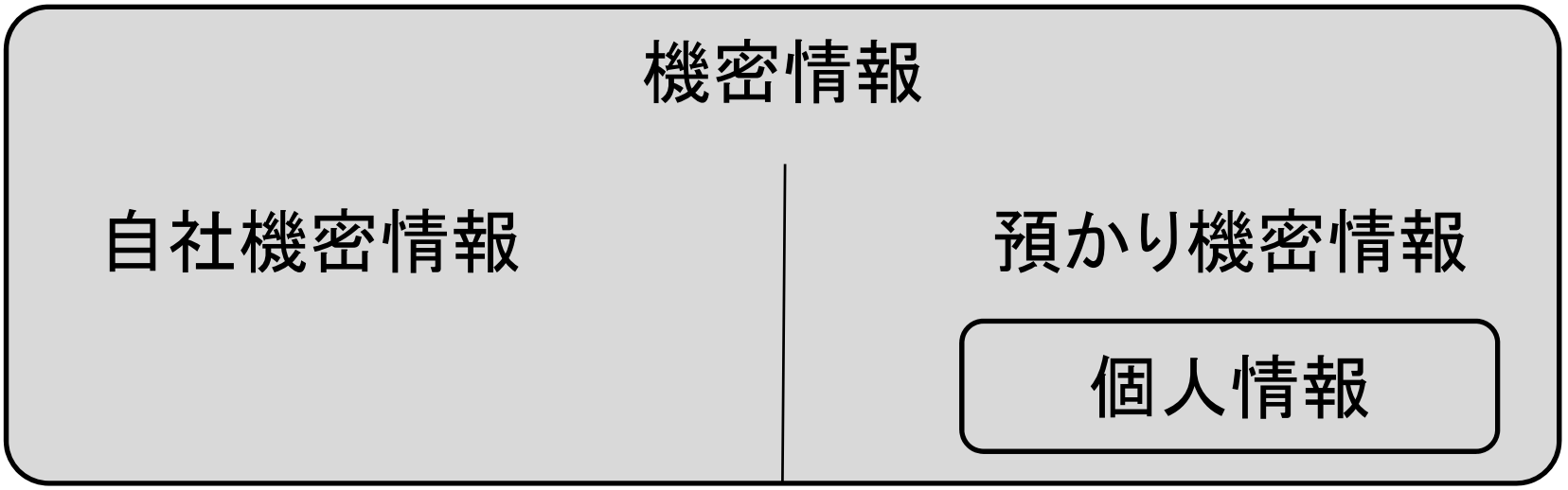
HPにおけるプライバシーとセキュリティ対策
Business enabler としてのチェイン



日本ヒューレット・パッカード株式会社 ©2010-2012

個人情報は　預かり機密情報　として取り扱う

・機密情報には、大きく分けて、自分の情報と、他から預かっている情報の２種類がある。



参考：機密情報とは

http://bit.ly/kimitsujouhou

http://yoshihiro.cocolog-nifty.com/security/2004/12/post_2.html

日本ヒューレット・パッカード株式会社 ©2010-2012

機密保持契約書 と 個人情報保護契約書における機密保持条項 との違い

機密保持契約書
- 機密情報を提供者が特定
- 業務達成目的の範囲内で関係者の取り扱いを許容
- 業務達成目的の範囲内で主体的に利活用される

個人情報保護契約における機密保持
- 個人情報を受領者が認識
- 取り扱い者は業務の直接従事者に制限
- 主体的な利用は一切禁止

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報の保管
HP秘(HP Confidential)としての対策

HP業務外秘(HP Restricted)としての対策は不十分である点に注意。

・アクセス制限が必須

・社外通信は暗号化（S/MIME）が必須

→パスワード保護は条件によっては不十分

詳細については、社内個人情報保護ガイドラインを参照。

日本ヒューレット・パッカード株式会社 ©2010-2012

個人情報の利用
（お客様情報を使ったプロモーション）

日本ヒューレット・パッカード株式会社 ©2010

お客様情報を使ったプロモーション
データ抽出・照合

Privacy preference（＝オプトアウト＆オプトイン）の確認

オプトアウト（利用停止）の有無の確認

お客様の連絡先（住所、電話番号、電子メールアドレス、FAX番号）について、オプトアウトの申し出がないことを確認しなければならない。

オプトインの状態の確認

*電子メールアドレスとFAX番号については、オプトインを得ていること*を確認しなければならない。

プロモーションに使えないデータベース

Privacy preferenceの管理機能のないデータベースにあるお客様情報はプロモーションに使ってはならない。

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報を使ったプロモーション データ抽出・照合

Privacy preference（＝オプトアウト＆オプトイン）の値（フラッグ）と状態

Y (Yes)：明示的オプトインを得た

N (No)：オプトインを拒否された　又は
オプトアウトされた

U (Unknown)：オプトインの確認をしていない

I (Isolated)：データの削除要求をされた

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報を使ったプロモーション
コンタクト・ポリシーの管理

住所（*YまたはUにコンタクト可能*）

DM（郵送によるダイレクトメール）

→担当者許可制　＋　送付届出制

電話番号（*YまたはUにコンタクト可能*）

テレセールス（テレマーケティング）

→ガイドライン遵守

電子メールアドレス（*Yのみにコンタクト可能*）　※オプトイン必要

eDM（電子メールによるダイレクトメール）

→原則として発行を集約

FAX番号（*Yのみにコンタクト可能*）　*※オプトイン必要*

FAX送信によるセールスや案内

→（ガイドライン作成中）

日本ヒューレット・パッカード株式会社 ©2010-2012

お客様情報を使ったプロモーション
データ更新

お客様からのフィードバックを適時かつ正確にデータ更新すること。

登録データの変更（住所変更など）

利用停止（＝オプトアウト）状態の更新

お客様からの「～～してください。」という依頼については、「HPとして、～～させていただきます。」と受け止めること。

→「自分又は自部署が～～する」のでは不十分な点に注意すること。

日本ヒューレット・パッカード株式会社 ©2010-2012

SUPPORT ANGELS
NEXT
starring 4KB48

SUPPORT ANGELS
NEXT
starring 4KB48

ココロ オドル タッチ

Study team report on Privacy/Personal information Management system

Rapporteurs:
Heung Youl Youm / KR
John Phillips / UK
Matthieu Grall / FR
Yoshihiro Satoh / JP

Study team meetings

Using HALO – a video conferencing system

Thanks to Microsoft and Hewlett-Packard

1. Summary of JP position

Positions	AU	CA	EE	FR	GE	JP	KR	UK
Is there a need for a new personal information specific management system(PIMS)?						No		
If it is created, then is it preferable to:								
-develop new personal information specific security requirements (new scheme)								
-develop new personal information specific requirements (new scheme)								
-leverage existing security requirements (using the ISO/IEC 27001 scheme)						x		
-include whole set of standards including management system, controls (security and data protection) and guidelines								
If controls standard is created, then is it preferable to develop:Is there a need for new personal information specific controls?								
-Separated security controls and data protection controls as a part of multi parts PIMS								
-application specific standard based of 27002-Separated Controls (new scheme)?						x		
-add new controls to existing 27002								

"x" stands for "acceptable"

2. Summary of JP contribution

日本は、法執行がある国においては、法的要求事項と重複するマネジメントシステム規格の作成は有益ではないと想定している。
なぜなら、法が要求している対策は確実に達成しなければならないものであって、マネジメントシステムのライフサイクルによって改善されるべき対象のようなものではないからである。
組織がそのようなマネジメントシステムの認証取得を試みたが、対策のいずれかが達成されていなかったという理由で失敗になった時に、それが何を意味するのかについても関心のあるところである。それは、その時点で組織が違法状態であったことを意味するのだろうか？組織にとってそのような認証を取得することの動機付けは何になるのだろうか？
しかしながら、それが国際規格としてやはり有益であり、それを作成することが決定されるのであれば、日本はISO/IEC 27001を用いて、"任意"の管理策セットという新しいスキームによって、ISO/IEC 27002にプライバシー管理策を追加することをハイライトする。
管理策群は、29100（のライフサイクルの考え方を用い、かつ、セキュリティ管理策を除く）をもとにした独立したものであるべきであり／あることができる。
日本は（マネジメントシステム規格を新たに作成しなくても）組織にPIMSを構築することができるNWIPの案を用意したが、日本はそれ（このような作成）がやはり有益であると決定されない限り、その提案をするつもりはない点について留意していただきたい。

ISMSユーザーズガイド「1．2適用」(10～11ページ)

ISMS認証基準及び附属書A「管理目的及び管理策」に規定された要求事項の適用を除外する場合は、原則的に組織の実施するリスクアセスメントの結果に基づき、経営陣や責任者の判断により正式にリスクの受容が決定されたことを示す証拠を、適用宣言書に合理的な理由と併せて明記する必要があります。

～中略～

安易な適用除外は、マネジメントシステムの一貫性に大きな影響を与えます。

以下に例示するような「除外の原則」を定め、ある要求事項について条件が全て満たされる場合にのみ適用を除外するなど公正な判断が求められます。

- ISMSの能力、責任に影響を及ぼさないこと
- ISMSの目標と相反しないこと
- 関連法規や規制に関する要求事項でないこと

http://www.isms.jipdec.jp/doc/JIP-ISMS111-21_2.pdf

本日のアンケート

◎以下のアンケートにお答えください。

■設問４：情報セキュリティ対策と個人情報保護対策の違いについてご存知でしたか？
１．理解していた　２．ある程度理解していた　３．あまり理解していなかった
４．初めて理解した

■設問５：個人情報保護マネジメントシステムの国際規格は必要だと思いますか？
１．はい　２．いいえ　３．どちらともいえない

◎設問５で「２」又は「３」を選んだ方は、設問９に進んでください。

本日のアンケート

■設問６：ISMS（ISO/IEC 27001）規格とどのような関係で国際規格ができるとよいと思いますか？
１．ISO/IEC 27001に必須項目として取り入れる（ISMS認証取得では必須になります）
２．ISO/IEC 27001に任意選択項目として取り入れる（ISMS認証取得に種類ができることになります）
３．ISO/IEC 27001とは異なる規格として新規作成する
■設問７：情報セキュリティ対策をどのように位置付ける構成の国際規格がよいと思いますか？
１．情報セキュリティ対策を直接的に含める国際規格
２．情報セキュリティ対策を他の規格の参照を求めるなど間接的に含める国際規格
３．情報セキュリティ対策を含めない国際規格（情報セキュリティ対策は、この規格とは別途実施すべきことであるという使い方）
■設問８：国内法との関係をどのようにする内容の国際規格がよいと思いますか？
１．必須の要求事項を定めずに、それを必須とするかは国内法令等の要求に従うことを定める国際規格（結果的に、国内法令等と同じ要求事項のレベルになる）
２．必須の要求事項を定める国際規格。国際規格が必須としない事項のうち国内法令等が要求している事項は、法令等遵守として実施することを想定する。（結果的に、国内法令等より高い要求事項のレベルになる）
３．その他：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本日のアンケート

■設問９：仮に、個人情報保護マネジメントシステムの国際規格が発行された場合に、国内の
JIS Q 15001規格はどうなるのがよいと思いますか？
１．国際規格に合わせて改訂するのがよい
２．このままにして、国際規格対応の国内規格については別途作成するのがよい
３．その他：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

■設問１０：仮に、個人情報保護マネジメントシステムの国際規格が発行された場合に、国内の
プライバシーマーク制度はどうなるのがよいと思いますか？
１．国際規格に合わせた制度として見直すのがよい
２．このままにして、国際規格対応の制度については別途作成するのがよい
３．その他：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本日のアンケート

◎表面ページの設問６で「３」を選び、設問７で「１」を選んだ方は、以下の設問１１にお答えください。

■設問１１：仮に、個人情報保護マネジメントシステムの国際規格が設問６の「３」及び設問７の「１」のような内容で発行された場合に、現状のISO/IEC 27001の中にある個人情報保護の項目はどのようにするのがよいと思いますか？

１．現状のままでよい
２．新しくできる国際規格を参照することを求めるように変えるのがよい
３．削除する（新しくできる国際規格で対策すればよい）